U.S. Express Mail No.: ER 023609497 US
Filing Date: February 6, 2004

PATENT
Howrey Matter No. 02453.0019.NPUS00
Extreme Docket No.: P107

METHOD AND SYSTEM FOR LOCATION-BASED ACCESS CONTROL IN A COMPUTER NETWORK

INVENTORS

SHEHZAD T. MERCHANT

MANISH M. RATHI

RELATED APPLICATIONS

This application is related to U.S. Patent Application No. To Be Determined, Howrey Docket No. 02453.0020.NPUS00, entitled "Apparatus, Method And System For Improving Network Security"; U.S. Patent Application Serial No. To Be Determined, Howrey Docket No. 02453.0021.NPUS00, entitled "Unified Adaptive Network Architecture." Each of the foregoing applications is filed concurrently herewith, and owned in common by the assignee hereof. Moreover, each of these applications is fully incorporated herein by reference as though set forth in full.

FIELD OF THE INVENTION

The invention relates generally to computer networks, and more specifically, to a network that includes mechanisms for regulating user access to the network.

BACKGROUND OF THE INVENTION

Computer security, particularly network security, has become a significant concern in recent years. Network security concerns generally fall into two categories: privacy and access control. Privacy mechanisms are used on networks to prevent the publication of otherwise private information; while access control protocols are designed to prevent unauthorized access to computer networks and the information stored on computers connected to the networks. Without access control features in place, unauthorized users can access a network and steal or corrupt stored information, or disrupt operation of the network. Unauthorized access is of particular concern on

networks that provide access to sensitive information, e.g., those used in enterprise environments, such as corporations or government entities.

Industry standards have been created to address the need for improved computer network security. The IEEE 802.1x standard is becoming a popular access control mechanism for contemporary wired and wireless local area networks (LANs). The 802.1x standard provides access control based on a variety of known authentication mechanisms including TLS, TTLS, MD5, and the like. Using any of these mechanisms, authentication is done based on the client's identity, be it a user name/password, certificates, or some other identification indicia. The authentication is typically performed by a back-end authentication server, which validates the user's identity and permits or denies access to the network based on the result of that validation, as well as other local policy decisions.

If the user is permitted access, the user can attach to and access the network from essentially any network attachment point. While the attachment point is traditionally an Ethernet switch port, it could also be a wireless LAN access point (AP), such as a Wi-Fi AP, or any other network attachment point.

In a conventional 802.1x LAN environment, as the user moves from location to location within the network, the user is typically allowed to access the network, so long as the user's identity is authenticated correctly using the back-end authentication infrastructure. There is no notion of restricting the user's access based on his/her physical location.

The ability to restrict network access based on the user's location would be highly desirable in some situations. For example, it may be desirable to create a campus or enterprise network having different zones that have different levels of security. In this type of network, a user that is allowed access to only a less secure zone should be denied access to a more secure zone. The ability to conveniently enforce different security levels for different zones of a network would be particularly desirable in a wireless LAN environment, where mobile users can easily move between locations in the network. In these environments, an unauthorized user could readily gain access to a higher security zone by simply moving his/her wireless terminal within range of an attachment point

within the zone. Accordingly, there is a need for a location-based access control scheme that can be conveniently incorporated into the existing authentication infrastructure of a network.

SUMMARY OF THE INVENTION

It is an advantage of the invention to provide a network system for controlling access to a computer network based on both location and client identity (e.g., user identity and/or user station identity).

In accordance with an exemplary embodiment of the invention, the system includes a network switch for requesting a client identity from a user station when it attempts to connect to the network. Upon receiving the client identity, the switch associates location information with the user identity. The location information can represent the physical location of a port of the switch, or alternatively, the location of a network edge device, such as an AP that communicates with the user's station over a wireless channel. The client identity and associated location information are then passed to an authentication server. The authentication server authenticates the client identity and compares the location information against a policy designating locations, if any, at which the user is permitted to connect to the network. The server then decides whether to grant or deny the user access to the network based on the authenticity of the client identity and the comparison of the location information. This architecture allows a campus-wide network to be segregated into zones having different levels of access security, and is particularly useful in wireless data networks, such as Wi-Fi environments.

In accordance with another exemplary embodiment of the invention, a network includes a plurality of edge devices for communicating with a plurality of user stations over one or more wireless channels. Within the network, the edge devices are connected to the ports of a network switch. A software application running on each of the edge devices requests identities from the user stations when they attempt to connect to the network. In addition, the application also associates location information with each of the client identities. The identities and associated

location information are then transferred to an authentication server. The authentication server decides whether to grant or deny each of the user stations access to the network based on the corresponding client identity and location information. This decision is then passed back to the switch, which either blocks or permits the client to connect to the network.

Method counterparts to these embodiments are also provided. Other embodiments, systems, methods, features and advantages of the invention will be or will become apparent to one with skill in the art upon examination of the following figures and detailed description. It is intended that all such additional embodiments, systems, methods, features and advantages be included within the scope of the invention, and be protected by the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The components in the figures are not necessarily to scale, emphasis instead being placed upon illustrating the principles of the invention. In the figures, like reference numerals designate corresponding parts throughout the different views.

FIG. 1 is a conceptual diagram of an exemplary computer network in accordance with an embodiment of the present invention.

FIG. 2 illustrates an example of a policy table for designating locations accessible by various users.

FIG. 3 is a flow chart illustrating a method of controlling access to the network of FIG. 1 in accordance with another embodiment of the invention.

FIG. 4 illustrates an exemplary dictionary file for establishing location information on a RADIUS server.

FIG. 5 illustrates an exemplary administrator interface of a configuration utility for setting user location attributes on a RADIUS server.

FIGS. 6A-C illustrate RADIUS message formats suitable for passing location and other information to a RADIUS server.

DETAILED DESCRIPTION

The description below, while illustrated and explained within the context of the IEEE 802.1x protocol, can be applicable more generally to other networks and protocols.

Turning now to the drawings, and in particular to FIG. 1, there is illustrated a network system 10 in accordance with an exemplary embodiment of the invention. The network 10 enhances an existing access control framework to include physical location as a decision criteria in determining if a client (i.e., user or user station) is allowed access to the network 10.

Using conventional access mechanisms, such as IEEE 802.1x, when an end user station attempts to connect to the network, an authenticator requests the identity of the user station. The identity information is passed back by the authenticator to an authentication server for authentication.

In contrast, using the presently disclosed system 10, the authenticator augments the identity of the client, which can be the user station identity, the user identity or both, and can include information such as a user name or password, certificates, media access control (MAC) address or some other identification indicia (credentials), with location information corresponding to the physical location of the client. The identity of the client along with the location information is passed back to the authentication server 14.

Policies 40 on the authentication server 14 are augmented to include location information. The authentication server 14 determines whether the client should be granted network access based on the authenticity of the client identity, and a comparison of the location information against policy table(s), which designate the locations, if any, at which the client is permitted to connect to the network 10.

The system 10 includes one or more network switches 12 that communicate with an authentication server 14 by way of the network 16.

A plurality of network edge devices 18a and wired user stations 18b are connected to the ports of the switches 12. Wireless edge devices 18a, such as wireless access points (APs), permit mobile user stations 22 to access the network over one or

more wireless channels. The edge devices and wired user stations 18a-b can be any electronic network devices capable of communicating with the network switches 12.

User stations 18b, 22 are devices that allow end users to log on onto the network and access its services. The wired devices 18b can be end user devices (user stations), such as personal computers, that directly connect to the switch ports using a wired connection, such as a standard Ethernet cable. Additionally or alternatively, wired edge devices, such as routers, bridges, or gateways that communicate with end user devices over other wired networks (not shown), instead of wireless channels, can be directly connected to the switch ports, in a manner similar to the connection of the wired user stations 18b.

A network manager 20 is optionally included in the system 10 for configuring the switches 12 and the authentication server 14. The network manager 20 can alternatively be connected directly with the switches 12 and server 14 to bypass the network 16. The network manager 20 can be a server running an application that permits a network administrator to configure the location information and software images stored in the switches 12. The application can also allow the administrator to create and update the policy table 40 in the authentication server 14.

The switches 12, authentication server 14, and network manager 20 can communicate with one another using any suitable access mechanism, such as SNMP, TELNET, TCP/IP, HTTP, or the like. Any suitable data network can be used to connect these components. Preferably, the data network 16 is an Ethernet network. In addition, the network 16 can also include other networking components (not shown), such as gateways, routers, additional servers hosting a variety of different applications, as well as links to other networks, such as an enterprise intranet or the public Internet.

Where the wireless edge device 18a is a wireless AP, it can provide network access to one or more wireless user devices 22, such as personal computers, lap tops, PDAs, phones, cameras, or the like. The wireless user devices 22 and the APs 18a can communicate using a conventional wireless protocol, such as a Wi-Fi protocol based on one of the IEEE 802.11 standards.

Each network switch 12 includes one or more ports corresponding to each of the network edge devices and wired user stations 18a-b. The ports (not shown) permit network communications between the edge devices and wired user stations 18a-b and the network 16. The network switch 12 can be a commercially-available local area network (LAN) Ethernet switch, configured to conform with the principles of the access control scheme disclosed herein.

Communications between the network 16 and the connected edge devices and wire user stations 18a-b pass through the switches 12. The switches 12 can be deployed in secure wiring closets in a campus environment.

Each switch 12 includes software 26 and hardware (not shown) for managing and forwarding traffic between the wireless edge devices and wired user stations.. Each switch 12 can also include a memory for storing location information. The location information can include indicia of the switch's location, and can also or alternatively include the locations corresponding to each of its ports. When the location information is associated with a particular port, it can indicate the physical location of the edge device or wired user station 18a-b connected to the port.

The application 26 has interface software for allowing an administrator to create and/or update the stored location information using the network manager 20. The location information is preferably in the form of ASCII text, but can also be any identifier suitable for indicating the location of the user or edge device being authenticated.

Preferably, an authenticator 27 resides on each of the wireless edge devices 18a. The authenticator 27 is for receiving and forwarding client credentials (user and/or user station credentials) and location information to the authentication server 14. The authenticator 27 is preferably an authenticator operating in conformance with the IEEE 802.1x standard. When a user on a wireless end user station 22 attempts to log onto the network, the authenticator 27 requests the user station and/or user's credentials. To verify the credentials of a client attempting to access the network, the authenticator 27 uses the authentication server 14. The authentication server checks the credentials of the client on behalf of the authenticator 27, and then responds to the

authenticator 27, indicating whether or not the client is authorized to access the services available through the switch 12. In this arrangement, location information is stored in the respective edge device 18a, indicating the physical location of the edge device. The authenticator 27 communicates with the authentication server 14 via the switch 12.

Alternatively/additionally, an authenticator can be located in each of the switches 12. In this arrangement, the authenticators function in essentially the same manner as the edge device based authenticator 27. The switch-based authenticator can be used to authenticate the client identities received from the edge devices 18A, the wired user stations 18b, and the end user stations 22 when they attempt to connect to the switch 12.

Any suitable network protocol, such as a data packet scheme, can be used for communications between the network switches 12 and respective edge devices and wired user stations 18a-b. Preferably, Ethernet is used to communicate messages and information between the switches 12 and the connected devices 18a-b.

The authentication server 14 can be a commercially-available Remote Authentication Dial-In User Service (RADIUS) server that is configured to provide authentication and access control services in accordance with the invention as described herein, and preferably conforms with the operational principles of the industry standard RADIUS protocol. Preferably, the switches 12 use the RADIUS protocol to forward the connection attempt parameters to the server 14 and receive the connection authorization responses.

Preferably, the authentication server 14 runs Steel-Belted Radius, Enterprise Edition available from Funk Software, Inc. of Cambridge, MA.

Although an authentication server 14 is shown, a more general policy server that authenticates and implements access control and other security policies could be equivalently used in the system 10. In alternative embodiments, the authentication server 14 can be included as a component in one or more of the switches 12, instead of a stand-alone server, as shown.

Fig. 2 is an exemplary table 40 illustrating a policy designating locations at which various end users are permitted to access the network. The policy table 40 can be a MIB or any equivalent data structure accessible by the authentication server 14. The table 40 associates user identities with their authorized access locations. In the example shown, User 1 is allowed to connect to the network at Locations 1, 3, and 5-7. User 2 is allowed to access the network when he/she is connected at either location 2 or 9; User 3 is allowed to access the network from Locations 1-9; and User N is permitted network access at location 7 and 9.

A similar policy table designating locations at which user stations (wireless and/or wired) are permitted to access the network can also be included in the authentication server 14. The user station table associates user station identities with their authorized access locations. By including both tables in the authentication server 14, location based access can be granted based on the user identity, user station identity, or a combination of both user identity and user station identity.

Tables associating other client identifiers with location information can also be included in the authentication server 14.

A network administrator configures the authentication server 14 with the location based access information in addition to user identity, user station identity and other information. Using Steel-Belted Radius, dictionary files are used by an administrator to establish checklist RADIUS attributes. These attributes designate information, such as location information and user credentials, used by the authentication server 14 to authenticate a client attempting to connect to the network 10. Fig. 4 illustrates an exemplary dictionary file for establishing user location (vendor specific attribute type 208) as a checklist attribute on the Steel-Belted Radius server.

Fig. 5 illustrates using the Steel-Belted configuration utility to set the value of the user location attribute for a particular user. In the example shown, the value is a string indicating one or more locations at which the user is allowed to access the network. The value is stored at the authentication server 14. As discussed below in greater detail, the stored value is checked against the location value sent by the

authenticator during a logon session. If there is a match, the user is permitted network access. Otherwise network access is denied.

Fig. 3 is a flowchart 50 illustrating a method of controlling wireless user access to the network 10 of Fig. 1. The method is described using authentication of the user's identity as an example. However, the scope of the invention covers network access regulation of other types of clients, such as user stations, wired users and wired user stations. Authentication can be based not only on user identity, but also user station identity, the combination of user identity and user station identity or any other client identifier. Thus, in the method discussed below, user identity can be substituted with client identity to generally apply the method to other types of clients.

Turning now to the method, when a wireless user at a user station 22 attempts to connect to the network 10, the authenticator 27 in the wireless edge device 18a handling the connection requests an identifier from the user (step 52). The user identity can be any suitable credential, such as a user name, password, certificate, media access control (MAC) address, shared encryption key, a smart card identifier, or any combination of the foregoing.

Upon receiving the user identity, the network switch 12 associates location information with the user identity (step 54). The location information can be a text string indicating the physical location of the switch 12. Alternatively, the location information can indicate the location of the edge device 18a through which the user is attempting to connect to the network. The location information can be stored locally on the edge device 18 or on the switch 12. When stored on the switch 12, it can be updated by the network manager 20, and periodically downloaded to the edge devices 18a. The switch 12 can store a table of locations, wherein each location corresponds to a switch port that is attached a wireless edge device 18a. The network manager 20 can include an application for allowing a network administrator to populate and update the location table.

The authenticator 27 in the wireless edge device 18a then passes the user identity and associated location through the switch 12 and over the network 16 to the authentication server 14. When a RADIUS server is used as the authentication server

14, this information is forwarded using a standard RADIUS access request message comprised of standard RADIUS attributes, such as user-name, user-password, NAS-IP-address (which is set to the address of the switch 12), service-type (value = login(1)), calling-station-ID (value = media access control (MAC) address of the user station), and NAS-port (value = switch port ID that the edge device is connect to) and vendor specific attributes. The location information is included as a RADIUS vendor specific attribute.

Figs. 6A-C illustrate the RADIUS message format. Fig. 6A shows the overall RADIUS message format, as defined by the RADIUS protocol. A RADIUS message comprises a code, identifier, length, authenticator, and one or more attributes. The attributes can be standard RADIUS attributes or vendor specific attributes. When the code is set to 1, this designates an access request packet.

The RADIUS attributes of the access request packet are defined as type length values (TLVs) that contain additional information, as shown in Fig. 6B.

Vendor specific attributes (VSAs) indicate a vendor ID, such as 1916, and a sting field encoding a sequence of one or more vendor TLVs, as shown in Fig. 6C.

As an example, a RADIUS access request packet supporting location-based authentication can contain the following TLVs:

Type	Length	Value
4 (NAS-IP)	4	192.168.0.1
87 (NAS Port)	5	1:4
26 (VSA)	xx	1916

TABLE 1

The vendor attribute 1916 is followed by VSA information. For user location, the vendor-attribute-type is 208, followed by the length of the location attribute, and the attribute value, such as "Cafeteria". The length xx is the length of the entire VSA, including the TLVs of the specific attributes.

After receiving the information from the authenticator 27, the authentication server 14 then authenticates the user identity (step 56). The authentication server 14

can use standard mechanisms, such as TLS, TTLS, EAP-TLS, EAP-TTLS, MD5, or the like, or combinations of the foregoing, to establish the authenticity of the user. Other authentication schemes can be used, and the invention is not limited to those previously listed. With the exemplary RADIUS access request described above in TABLE 1, the authentication is based on the user-name and user-password attributes.

If the authentication fails, the user is denied access to the network (step 62). If, on the other hand, the user is correctly authenticated, the authentication server 14 determines whether the user is allowed access at the location indicated by the location information. This is done by comparing the location information in the VSA against the respective policy table (or checklist attributes) designating the locations, if any, at which the user is permitted to connect to the network 10 (step 58).

If the user is permitted access at the indicated location, the authentication server 14 transmits a message to the respective switch 12 granting network access to the user (step 60). If the user is not permitted access at the indicated location, the authentication server 14 so notifies the switch 12, and the user is denied network access (step 62). When a RADIUS server is used as the authentication server 14, these messages are transmitted to the switch 12 using standard RADIUS messages.

For users attempting to access the network using the wired user stations 18b, the above procedure described in connection with Fig. 3 is used, with the authenticator residing on the switch 12.

In a wireless LAN environment, as a user moves away from the access point he/she is currently associated with, depending on how his client network interface card (NIC) operates in the user device 22, the wireless signal strength from the AP he/she is currently associate with will deteriorate. At some point the client NIC driver will completely lose the signal from the current AP and start scanning for another AP, or it may proactively start scanning for another stronger signal. If another AP is found whose received signal strength is stronger than the current one and the configuration parameters match, the client NIC will try to associate and authenticate with the new AP. When the client tries to authenticate to the new AP, the new AP will include its location information along with any user and/or user

station credentials supplied by the client to re-authenticate the client to the new AP using the scheme described above.

In this manner, a wireless user station can roam from one network point of attachment to another in a campus or enterprise environment and the location-based security policy disclosed herein can be enforced. The client's new location is passed back to the authentication server by the authenticator residing in the network point of attachment, i.e. the AP. The authentication server re-authenticates the client and uses its new location information along with other policies to determine if the client is allowed access to the network at the new location.

In an alternative embodiment of the invention, a user or his/her station could be authenticated the first time he/she attempts to connect to the network. If the user is permitted access based on the location, its authenticity and/or other policies, the client is allowed to access the network. If the client moves to another location on the network, the authentication step can be skipped and the location of the client and/or other policies is used to determine if the client is allowed access to the network.

Using the access mechanism disclosed herein, an administrator could use the physical location of the client's network point of attachment, along with authentication of the client and other administrative policies, such as MAC-filtering, to allow or deny access to the network.

While various embodiments of the invention have been described, it will be apparent to those of ordinary skill in the art that many more embodiments and implementations are possible that are within the scope of this invention. For example, any combination of any of the systems or methods described in this disclosure are possible.

What is claimed is: